

Non-existence of two types of partial difference sets

S. De Winter ^{*} [†]E. Neubert ^{*} [‡]Z. Wang ^{*} [§]

Abstract

In this note we prove the non-existence of two types of partial difference sets in Abelian groups of order 216. This finalizes the classification of parameters for which a partial difference set of size at most 100 exists in an Abelian group.

Keywords— Partial difference set

1 Introduction

Let G be a finite Abelian group of order v . Then D is a (v, k, λ, μ) -*partial difference set* (PDS) in G if D is a k -subset of G with the property that the expressions gh^{-1} , $g, h \in D$, represent each non-identity element in D exactly λ times, and each non-identity element of G not in D exactly μ times. Further assume that $D^{(-1)} = D$ (where $D^{(s)} = \{g^s : g \in D\}$) and $e \notin D$, where e is the identity of G , then D is called a *regular* partial difference set. A regular PDS is called *trivial* if $D \cup \{e\}$ or $G \setminus \{D\}$ is a subgroup of G .

In [5] Ma presented a table of parameters for which the existence of a regular PDS with $k \leq 100$ in an Abelian group was known or could not be excluded. In particular the list contained 32 cases where (non)-existence was not known. In [7] Ma excluded the existence of a PDS in 13 of these 32 cases. In [3] and [4] existence was proved in one of the remaining cases, and recently De Winter, Kamischke and Wang [1] proved nonexistence for all but two of the remaining cases. These remaining cases were the possible existence of a $(216, 40, 4, 8)$ -PDS and a $(216, 43, 10, 8)$ -PDS in an Abelian group of order 216. In this note we will prove nonexistence of such PDS, hence finalizing the classification of parameters for which a PDS with $k \leq 100$ exists in

^{*}Michigan Technological University

[†]sgdewint@mtu.edu

[‡]ejneuber@mtu.edu

[§]zeying@mtu.edu

an Abelian group. The proof uses ideas developed in [1], but requires an additional argument based on weighing points and lines in a projective plane.

2 Preliminaries

The following three results will be used in our proof. The first two are due to Ma [5, 6], the third is a recent local multiplier theorem from [1].

Proposition 2.1 *No non-trivial PDS exists in*

- *an Abelian group G with a cyclic Sylow- p -subgroup and $o(G) \neq p$;*
- *an Abelian group G with a Sylow- p -subgroup isomorphic to $\mathbb{Z}_{p^s} \times \mathbb{Z}_{p^t}$ where $s \neq t$.*

Proposition 2.2 *Let D be a nontrivial regular (v, k, λ, μ) -PDS in an Abelian group G . Suppose $\Delta = (\lambda - \mu)^2 + 4(k - \mu)$ is a perfect square. If N is a subgroup of G such that $\gcd(|N|, |G|/|N|) = 1$ and $|G|/|N|$ is odd, then $D_1 = D \cap N$ is a (not necessarily non-trivial) regular $(v_1, k_1, \lambda_1, \mu_1)$ -PDS with*

$$|D_1| = \frac{1}{2} \left[|N| + \beta_1 \pm \sqrt{(|N| + \beta_1)^2 - (\Delta_1 - \beta_1^2)(|N| - 1)} \right].$$

Here $\Delta_1 = \pi^2$ with $\pi = \gcd(|N|, \sqrt{\Delta})$ and $\beta_1 = \beta - 2\theta\pi$ where $\beta = \lambda - \mu$ and θ is the integer satisfying $(2\theta - 1)\pi \leq \beta < (2\theta + 1)\pi$.

Proposition 2.3 [LMT] Let D be a regular (v, k, λ, μ) -PDS in an Abelian group G . Furthermore assume $\Delta = (\lambda - \mu)^2 + 4(k - \mu)$ is a perfect square. Then $g \in G$ belongs to D if and only if $g^s \in D$ for all s coprime with $o(g)$, the order of g .

3 The Main Result

Theorem 3.1 *There does not exist a $(216, 40, 4, 8)$ -PDS in an Abelian group.*

Proof. Assume by way of contradiction that D is a $(216, 40, 4, 8)$ -PDS in an Abelian group G of order 216. By Proposition 2.1, we know that $G \cong \mathbb{Z}_2^3 \times \mathbb{Z}_3^3$.

Let g_1, g_2, \dots, g_{26} be all elements of order 3 in G , and let $\mathcal{B}_{g_i} = \{ag_i \mid o(a) = 1 \text{ or } 2, ag_i \in D\}$, and $B_i = |\mathcal{B}_{g_i}|$, $i = 1, 2, \dots, 26$. That is, B_i equals the number of elements in D whose fourth power equals g_i .

Now observe that the LMT implies that raising elements to the fifth power provides a bijection between \mathcal{B}_{g_i} and $\mathcal{B}_{g_i^2}$. Hence $|\mathcal{B}_{g_i}| = |\mathcal{B}_{g_i^2}|$.

Let N be the Sylow-2-subgroup of G . Using Proposition 2.2 we obtain that $|N \cap D| = 0$ or 4. First assume that D contains no elements of order 2. We see that $\Sigma_i B_i = 40$ and $\Sigma_i B_i(B_i - 1) = 56$, where the latter equality follows as all 7 elements of order 2 are not in D , and thus each have exactly $\mu = 8$ difference representations.

By relabeling the g_i if necessary, we may assume that $C_j := B_{2j-1} = B_{2j}$, for $j = 1, 2, \dots, 13$, and $C_1 \geq C_2 \geq \dots \geq C_{13}$. We now obtain

$$\Sigma_j C_j = 20 \quad \text{and} \quad \Sigma_j C_j^2 = 48. \quad (1)$$

It is easy to check that the system of equations (1) exactly has the following nonnegative integer solutions, listed as 13 tuples $(C_1, C_2, \dots, C_{13})$:

$$\begin{aligned} &(5, 3, 2, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1), \quad (5, 2, 2, 2, 2, 1, 1, 1, 1, 1, 1, 1, 0), \\ &(4, 4, 2, 2, 1, 1, 1, 1, 1, 1, 1, 1, 0), \quad (4, 3, 3, 2, 2, 1, 1, 1, 1, 1, 1, 0, 0), \\ &(4, 3, 2, 2, 2, 2, 2, 1, 1, 1, 0, 0, 0), \quad (4, 2, 2, 2, 2, 2, 2, 2, 2, 0, 0, 0, 0), \\ &(3, 3, 3, 3, 2, 2, 1, 1, 1, 1, 0, 0, 0), \quad (3, 3, 3, 2, 2, 2, 2, 2, 1, 0, 0, 0, 0). \end{aligned}$$

Secondly assume that D contains 4 elements of order 2. It follows that $\Sigma_i B_i + 4 = 40$. By counting the number of ways elements of order 2 can be written as differences of elements of D , we obtain that $\Sigma_i B_i(B_i - 1) + 4 \cdot 3 = 4 \cdot 4 + 3 \cdot 8$. Using similar labeling as above, we now obtain

$$\Sigma_j C_j = 18 \quad \text{and} \quad \Sigma_j C_j^2 = 32. \quad (2)$$

It is easy to check that the system of equations (2) has the following nonnegative integer solutions:

$$\begin{aligned} &(3, 3, 2, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1), \quad (3, 2, 2, 2, 2, 1, 1, 1, 1, 1, 1, 1, 0), \\ &(2, 2, 2, 2, 2, 2, 2, 1, 1, 1, 1, 0, 0). \end{aligned}$$

Recall that N is the unique subgroup isomorphic to \mathbb{Z}_2^3 in G . Let P_1, \dots, P_{13} be the 13 subgroups of G isomorphic to \mathbb{Z}_3 , and let L_1, \dots, L_{13} be the 13 subgroups of G isomorphic to \mathbb{Z}_3^2 . Now consider the incidence structure \mathcal{P} with points the subgroups $P_i \times N$, $i = 1, \dots, 13$, of G , with blocks the subgroups $L_i \times N$, $i = 1, \dots, 13$, of G , and with containment as incidence. Then it is easily seen that \mathcal{P} is a $2 - (13, 4, 1)$ design, or equivalently, the unique projective plane of order 3. We next assign a weight to each point of \mathcal{P} in the following way: if point p corresponds to subgroup $P_i \times N$ then the weight of p is $\frac{1}{2}|((P_i \times N) \setminus N) \cap D|$. In this way the weights of the 13 points of \mathcal{P} correspond to the 13 values C_1, C_2, \dots, C_{13} , that is, half of the number of elements of order 3 or 6 from D in the subgroup underlying the given point. Without loss of generality we may assume the labeling is such that point $P_i \times N$ has weight C_i . The weight of a block will simply be the sum of the weights of the points in that block.

We next count how many elements of order 3 or 6 from D a specific subgroup of the form $L_i \times N$ can contain. Assume that $|(L_i \times N) \cap D| = m$. Let ag and bh be two distinct elements from D , with $a^2 = b^2 = g^3 = h^3 = e$. Then $agh^{-1}b^{-1}$ belongs to $L_i \times N$ if and only if $gh^{-1} \in L_i$. It is easy to see that if $g \in L_i$ there are $m - 1$ possibilities for bh such that $gh^{-1} \in L_i$, whereas if $g \notin L_i$ there are $\frac{|D|-m-2}{2}$ possibilities for bh such that $gh^{-1} \in L_i$.

Counting the number of differences of elements of D that are in $L_i \times N$ in two ways, we obtain

$$m(m-1) + (k-m)\left(\frac{k-m-2}{2}\right) = \lambda m + \mu(71-m), \quad (3)$$

where $(k, \lambda, \mu) = (40, 4, 8)$. This yields that $m = 8$ or 16 .

Now define $m' := \frac{1}{2}|((L_i \times N) \setminus N) \cap D|$. We obtain the following table:

Case 1: (216, 40, 4, 8)-PDS	D contains 0 elements of order 2	$m' = 4$ or 8
Case 2: (216, 40, 4, 8)-PDS	D contains 4 elements of order 2	$m' = 2$ or 6

We now note that the values m' must be the weights of the blocks of \mathcal{P} , and that in both cases these weights are even. We first show that no value C_i can be odd. Assume by way of contradiction that C_i is odd for some i . Let the weight of the four blocks that contain $P_i \times N$ be n_1, \dots, n_4 respectively. Then

$$\sum_{j=1}^{13} C_j = C_i + \sum_{t=1}^4 (n_t - C_i),$$

which implies that $\sum_{j=1}^{13} C_j$ is odd, contradicting with the fact that $\sum_{j=1}^{13} C_j = 20$ or 18 .

This leaves us with only the possibility $(4, 2, 2, 2, 2, 2, 2, 2, 0, 0, 0, 0)$ for (C_1, \dots, C_{13}) in case 1. In this case, by considering the four blocks through a point with weight 2 it easily follows that it is not possible to distribute the thirteen given weights in such a way that every block has weight 4 or 8. This concludes the proof. \square

Theorem 3.2 *There does not exist a (216, 43, 10, 8)-PDS in an Abelian group.*

Proof. This case is dealt with in a very similar way. We will only provide a sketch of the proof. Assume by way of contradiction D is a (216, 43, 10, 8)-PDS in an Abelian group G .

As before $G \cong \mathbb{Z}_2^3 \times \mathbb{Z}_3^3$, and using Proposition 2.2 we obtain that D contains either 3 or 7 elements of order 2. If D contains 3 elements of order 2 we obtain

$$\Sigma_j C_j = 20 \quad \text{and} \quad \Sigma_j C_j^2 = 48 \quad (4)$$

which is the same as the system of equations in (1), and hence has the same set of solutions.

If D contains 7 elements of order 2 we obtain

$$\Sigma_j C_j = 18 \quad \text{and} \quad \Sigma_j C_j^2 = 32 \quad (5)$$

which is the same as the system of equations in (2), and thus has the same set of solutions.

With similar notation as in the previous theorem, and using the same counting argument for $(k, \lambda, \mu) = (43, 10, 8)$, one obtains $m = 11$ or 19 , and

Case 3: $(216, 43, 10, 8)$	D contains 3 elements of order 2	$m' = 4$ or 8
Case 4: $(216, 43, 10, 8)$	D contains 7 elements of order 2	$m' = 2$ or 6

As before the weights of all blocks of \mathcal{P} must be even, and the proof can be finished in the same way as in the $(216, 40, 4, 8)$ -PDS case. \square

4 Conclusions

It is interesting to note that no regular PDS exists in all but one of the cases that were originally left open in Ma's table [5]. The exception arising from a two-weight code in an elementary Abelian 2-group. Furthermore almost all known PDS in Abelian groups are of only few types: (negative) Latin square type, reversible difference sets, PCP type, Paley type, and projective two-weight sets. Also, recently it was shown that in Abelian groups of order $4p^2$, p an odd prime, every non-trivial PDS is either of PCP type or a sporadic example in an Abelian group of order 36 [2]. These observations raise the question as to whether new strong and more general non-existence results can be proved, and whether further classifications for PDS in Abelian groups are possible. It is important to note that the situation in non-Abelian groups is very different, and many more examples exist in those groups.

References

- [1] S. De Winter, E. Kamischke and Z. Wang, Automorphisms of strongly regular graphs with applications to partial difference sets, *Designs, Codes, Cryptogr.*, **79**, 471–485 (2016)

- [2] S. De Winter and Z. Wang, Classification of partial difference sets in Abelian groups of order $4p^2$, *Designs, Codes, Cryptogr.*, (2016). doi:10.1007/s10623-016-0280-x
- [3] F. Fiedler and M. Klin, A strongly regular graph with the parameters $(512, 73, 438, 12, 10)$ and its dual graph, *Preprint MATH-AL-7-1998*, Technische Universität Dresden, 23 pp. (1998)
- [4] A. Kohnert, Constructing two-weight codes with prescribed groups of automorphisms, *Discr. Appl. Math.* **155**, 1451-1457 (2007)
- [5] S.L. Ma, A survey of partial difference sets, *Designs, Codes, Cryptogr.* **4**, 221-261 (1994)
- [6] S. L. Ma, On subsets of partial difference sets, *Discrete Mathematics* **125**, 263-272 (1994)
- [7] S.L. Ma, Some necessary conditions on the parameters of partial difference sets, *J. Statist. Plann. Inference* **62**, 47-56 (1997)